UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,205	02/14/2000	Jun Kogure	826.1590/JDH	6229

21171   7590   12/04/2003

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/04/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _08 August 2000_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under _Ex parte Quayle_, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-10_ is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-10_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☒ All b)☐ Some * c)☐ None of:

       1.☒ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

     a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _3_.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Objections

1.   Claim 7 is objected to because of the following informalities: line 15 reads "... sores ..."

when it should read "... stores ...". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1-3 and 6-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Leppek

(5,933,501).

In reference to claims 1 and 8, Leppek suggests a data generating apparatus and computer

readable storage medium, comprising: an input device inputting a condition for designating a

finite field (column 4 lines 33-51); a generation device automatically generating expression data

of the finite field based on the inputted condition (column 4 lines 52-67); and an expression data

storage device storing the generated expression data (column 4 lines 7-23).

In reference to claim 9, Leppek suggests a data generating method, comprising:

designating a condition for designating a finite field (column 4 lines 33-51); automatically

generating expression data of the finite field based on the designated condition (column 4 lines

52-67); and supplying the generated expression data to a finite field operation apparatus (column

4 lines 7-23).

In reference to claim 10, Leppek suggests a data generating apparatus, comprising:

inputting means for inputting a condition for designating a finite field (column 4 lines 33-51);

generating means for automatically generating expression data of the finite field based on the

inputted condition; and expression data storing means for storing the generated expression data

(column 4 lines 52-67).

3.   Claims 2-7 are rejected as in claim 1.

Regarding claim 2, further comprising an operation device performing a finite field

operation based on the expression data stored in said expression data storage device (column 5

lines 34-52).

Regarding claim 3, wherein when a bit length of a prime number which describes the

finite field is inputted as the condition, said generation device automatically generates prime

number data corresponding to the bit length and stores the generated prime number data in said

expression data storage device. Leppek uses different encryption routines (column 4 lines 14-17)

one well known example is the RSA encryption routine, which uses random keys. The size of

the keys is a design choice. The keys are inherently developed using a random number

generator, which would generate them automatically

Regarding claim 6, further comprising a fixed data storage device storing one or more

pieces of predetermined expression data of a finite field (Fig. 2), said generation device stores

expression data of a finite field corresponding to the condition in said expression data storage

device if there is the expression data of a finite field corresponding to the condition in the fixed

data storage device, and said generation device automatically generates expression data of a

finite field corresponding to the condition if there is no expression data of a finite field

corresponding to the condition in the fixed data storage device (column 5 lines 6-18). The

generator, of the Leppek system, always constructs the expression from the access code data

using the stored information in the fixed storage such as 100.

Regarding claim 7, further comprising: a designation device designating expression data

of a finite field (column 5 lines 6-18); and a verifier device verifying whether the designated

expression data are suitable, the verifier device sores designated expression data in said

expression data storage device if the designated expression data are suitable, and the verifier

device asks the designation device for other expression data if the designated expression data are

not suitable (claim 5 lines 19-33). The supervisory encryption assembly manager processes the

sequence and therefore is responsible for verifying that the encryption process is carried out as

designed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

4.   Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek as

applied to claim 1 above, and further in view of Wright.

Leppek does not expressly disclose the generation of polynomial expressions

Regarding claim 4, Wright discloses a random polynomial generator wherein when an

extension degree which describes the finite field is inputted as the condition, said generation

device automatically generates irreducible polynomial data corresponding to the extension

degree and stores the irreducible polynomial data in said expression data storage device (part 2.1 page 2).

Regarding claim 5, The data generating apparatus according to claim 4, wherein when an instruction using an optimal normal basis is inputted, said generation device automatically generates irreducible polynomial data for an optimal normal basis corresponding to the extension degree and the irreducible polynomial data for an optimal normal basis in said expression data storage device. Leppek discloses storing the predetermined expression in storage 100, however Leppek does not expressly disclose the generation of polynomial expressions. Wright discloses the generation of polynomial expressions (part 2.1 page 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the polynomial generator as in Wright in the system of Leppek. One of ordinary skill in the art would have been motivated to do this because Leppek discloses the use of conventional encryption algorithms (column 4 lines 14-17) and Wright discloses a polynomial generator which is satisfactory and has already been proven (Introduction 1 page 1).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.
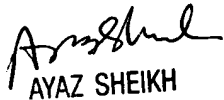
Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK
Friday, November 28, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100